DOI 10.37882/2223–2966.2022.09.38

ПРИМЕНЕНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ В КАЧЕСТВЕ ОДНОСТОРОННЕЙ ФУНКЦИИ С СЕКРЕТОМ

APPLIED ARTIFICAL NEURAL NETWORK AS A ONE-WAY FUNCTION WITH A SECRET

S. Tarasenko

Summary. This article discusses the mechanism of obtaining various output data from an artificial neural network of direct propagation with immutable input data by adding uniform noise when calculating the activation functions of some part of the neurons of the network. The mechanism proposed in this paper can be used to construct a cryptoprimitive having the properties of a one-way function with a secret, which in turn the queue allows you to build asymmetric cryptosystems based on it. The calculation of the cryptographic resistance of this function to the calculation of its prototype is also performed and graphs reflecting the weak correlations between input and output sequences are clearly demonstrated. The paper presents the arguments. On the basis of which it is possible to put forward a hypothesis about the applicability of this cryptoprimitive for constructing cryptographic algorithms based on it that are resistant to cryptanalysis using quantum computing. The results obtained in the course of this study may be of value when considering the mathematical aspects of asymmetric cryptography based on error correction in noise-resistant codes.

Keywords: noise-resistant coding, Hamming distance, artificial neural networks, one-way function with secret, asymmetric cryptography.

Тарасенко Сергей Сергеевич
Академия ФСО России (г. Орёл)
Dor7la96@mail.ru

Аннотация. В данной статье рассмотрен механизм получения различных выходных данных из искусственной нейронной сети прямого распространения при неизменяемых входных данных за счет добавления равномерного шума при вычислении значений функций активации некоторой части нейронов сети.

Предложенный в данной работе механизм может быть использован для построения криптопримитива, имеющего свойства односторонней функции с секретом, что в свою очередь позволяет строить на его основе ассиметричные криптосистемы. Также произведен расчет криптографической стойкости данной функции к вычислению ее прообраза и наглядно продемонстрированы графики, отражающие слабые корреляционные связи между входными и выходными последовательностями. В работе представлены доводы, на основе которых можно выдвинуть гипотезу о применимости данного криптопримитива для построения на его основе криптографических алгоритмов, устойчивых к криптоанализу с использование квантовых вычислений.

Результаты, полученные в ходе данного исследования, могут иметь ценность при рассмотрении математических аспектов асимметричной криптографии, основанной на исправлении ошибок в помехоустойчивых кодах.

Ключевые слова: помехоустойчивое кодирование, расстояние Хэмминга, искусственные нейронные сети, односторонняя функция с секретом, асимметричная криптография.

Введение

В настоящее время ведутся разработки криптографических алгоритмов асимметричной криптографии, основанные на вычислительной сложности решения NP-полных задач [1]. Существуют асимметричные криптосистемы, стойкость которых основана на вычислительной сложности решения задач дискретного логарифмирования [2] и факторизации больших целых чисел [3]. Появление алгоритма Питера Шора [4] для квантовых вычислительных машин, с помощью которых задачи дискретного логарифмирования и факторизации целых чисел могут быть решены за полиномиальное время [5], ставит под вопрос безопасность дальнейшего использования асимметричных криптосистем, основанных на данных проблемах теории чисел. Поэтому актуальным является вопрос модификации существующих способов построения криптосистем, устойчивых к криптоанализу с использованием вычислений на квантовом компьютере.

Различные реализации асимметричных криптосистем основываются на применении односторонних функций с секретом [6].

Пусть $\{0,1\}^n$ — множество всех двоичных строк длины n. Функция

$$f:\{0,1\}^* \to \{0,1\}^*$$

является односторонней функцией, если она эффективно вычисляется за полиномиальное время на детерминированной машине Тьюринга [7], но не существует полиномиальной вероятностной машины Тьюринга [8],

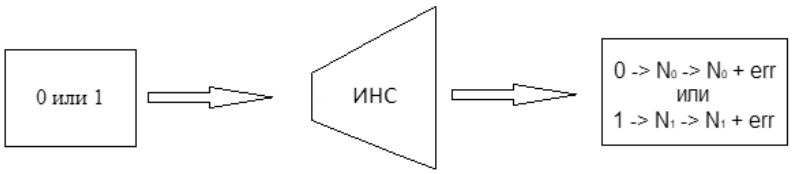


Рис. 1. Генерация нейронной сетью помехоустойчивых комбинаций с ошибками

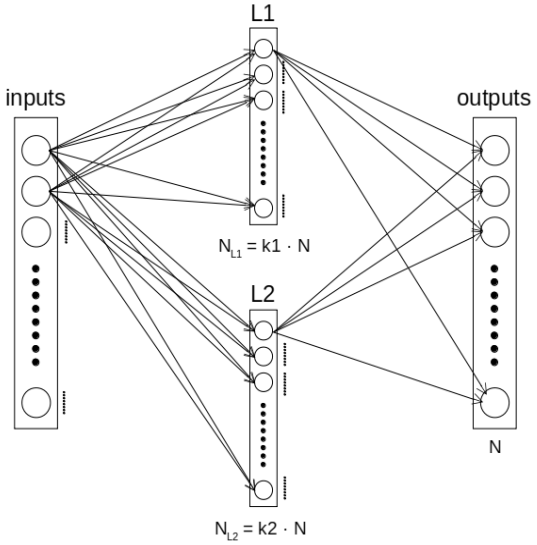


Рис. 2. Искусственная нейронная сеть прямого распространения

которая обращает эту функцию с более чем экспоненциально малой вероятностью. Для любой вероятностной полиномиальной машины V для любого полинома $p(n)$ и достаточно большого $n\in\mathbb{N}$ выполняется неравенство:

$$\Pr[V(f(m))\in f^{-1}(m)]<\frac{1}{p(n)}, \quad (1)$$

где строка m выбирается случайным образом на множестве $\{0,1\}^n$ в соответствии с равномерным законом распределения. Время работы машины V ограничено полиномом от длины искомого прообраза.

Односторонняя функция с секретом — функция дискретная, зависящая от параметра (секрета, описания секрета). Знание параметра позволяет эффективно (с полиномиальной сложностью) вычислять и инвертировать данную функцию. Если параметр неизвестен, то не существует эффективного алгоритма инвертирования функции. Семейство односторонних функций с секретом обладает свойствами односторонней функции.

В качестве односторонней функции с секретом предлагается использовать искусственную нейронную сеть прямого распространения [9], для части нейронов которой при вычислении значений функции активации добавляется равномерный шум [10].

Основная часть работы

Пусть существует M исходных последовательностей. Например, для M = 2 исходными последовательностями являются значения бит {0} и {1}. Им в соответствие ставятся M случайных N-битных помехоустойчивых кодовых последовательностей, удовлетворяющих условию [11]:

$$d_{\min} \geq 2\cdot t+1, \quad (2)$$

где $d_{\min}$ — расстояние Хэмминга [12] между каждой из M N-битных помехоустойчивых кодовых последовательностей со всеми другими $M-1$ N-битными помехоустойчивыми кодовыми последовательностями, t — количество вносимых ошибок в помехоустойчивую кодовую последовательность.

Преобразование исходной последовательности в помехоустойчивую последовательность с ошибками

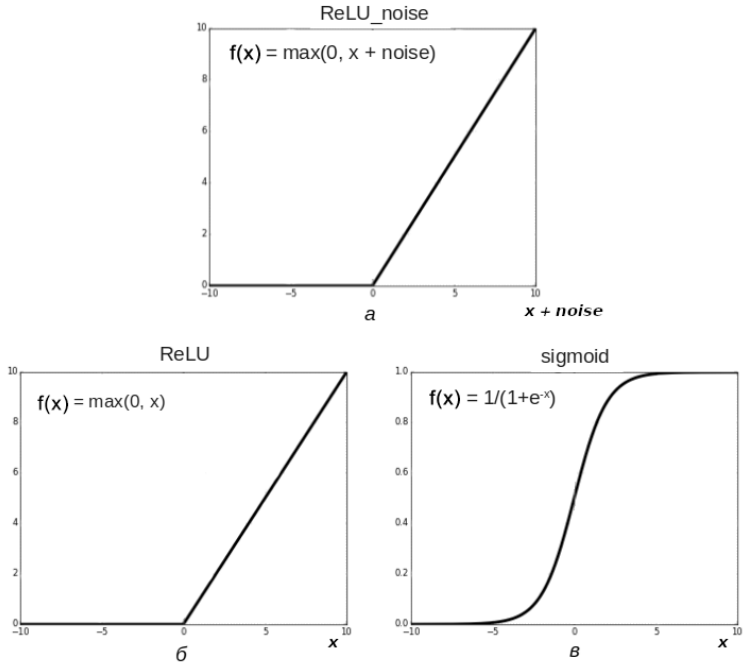


Рис. 3. Функции активации нейронной сети

можно осуществить с использованием искусственной нейронной сети (рис. 1), где N_0 — помехоустойчивая кодовая комбинация без ошибки для исходной последовательности {0}, N_1 — для {1}, err — вектор ошибок, ИНС –искусственная нейронная сеть прямого распространения. N_0 и N_1 являются секретом для предлагаемой односторонней функции, так как при знании их вычислительно легко определить исходную последовательность ({0} или {1}) используя нейронную сети Хопфилда, обученную на N_0 и N_1 [13].

Доказательство сходимости сети для решения данной задачи не требуется, так как при фиксированных наборах данных нейронная сеть «запоминает» все варианты и проблема обучения решается экстенсивным расширением нейронной сети путем увеличения скрытых слоев и количества нейронов в них.

Таким образом, N-битные помехоустойчивые кодовые последовательности, соответствующие M исходным последовательностям, являются результатом их преобразования искусственной нейронной сетью, выступающей в роли односторонней функции с секретом, которая может быть описана следующим образом.

Архитектура нейронной сети представлена на рисунке 2.

В слое $L1$ функция активации для всех нейронов представляет собой функцию $ReLU\_noise = ReLU(x + noise)$ при равновероятном распределении значений $noise$ на заданном интервале значений. (рис. 3, а):

$$f_1(x) = \max(0, x + noise). \quad (3)$$

В слое $L2$ функцией активации для всех нейронов является функция $ReLU$ [14] (рис. 3, б):

$$f_2(x) = \max(0, x). \quad (4)$$

$Inputs$ не является слоем как таковым и представлен на рисунке 2 для иллюстрации связи входного набора данных со слоями $L1$ и $L2$.

В слое $outputs$ функцией активации для всех нейронов является функция $sigmoid$ [15] (рис. 3, в):

$$f_3(x) = \frac{1}{1 + e^{-x}}. \quad (5)$$

Выходные данные из слоя $outputs$ округляются (если $f(x) \geq 0.5$, то $f(x) = 1$, если $f(x) < 0.5$, то $f(x) = 0$) и формируют последовательность длиной N бит, в которую внесено до t ошибок в сравнении с помехоустойчивым кодовым словом из N бит, соответствующими одной из M исходных последовательностей.

В ходе эксперимента было выявлено, что количество ошибок t, вносимых нейронной сетью, зависит от данных для обучения, а именно от расстояния Хэмминга между помехоустойчивыми кодовыми последо-

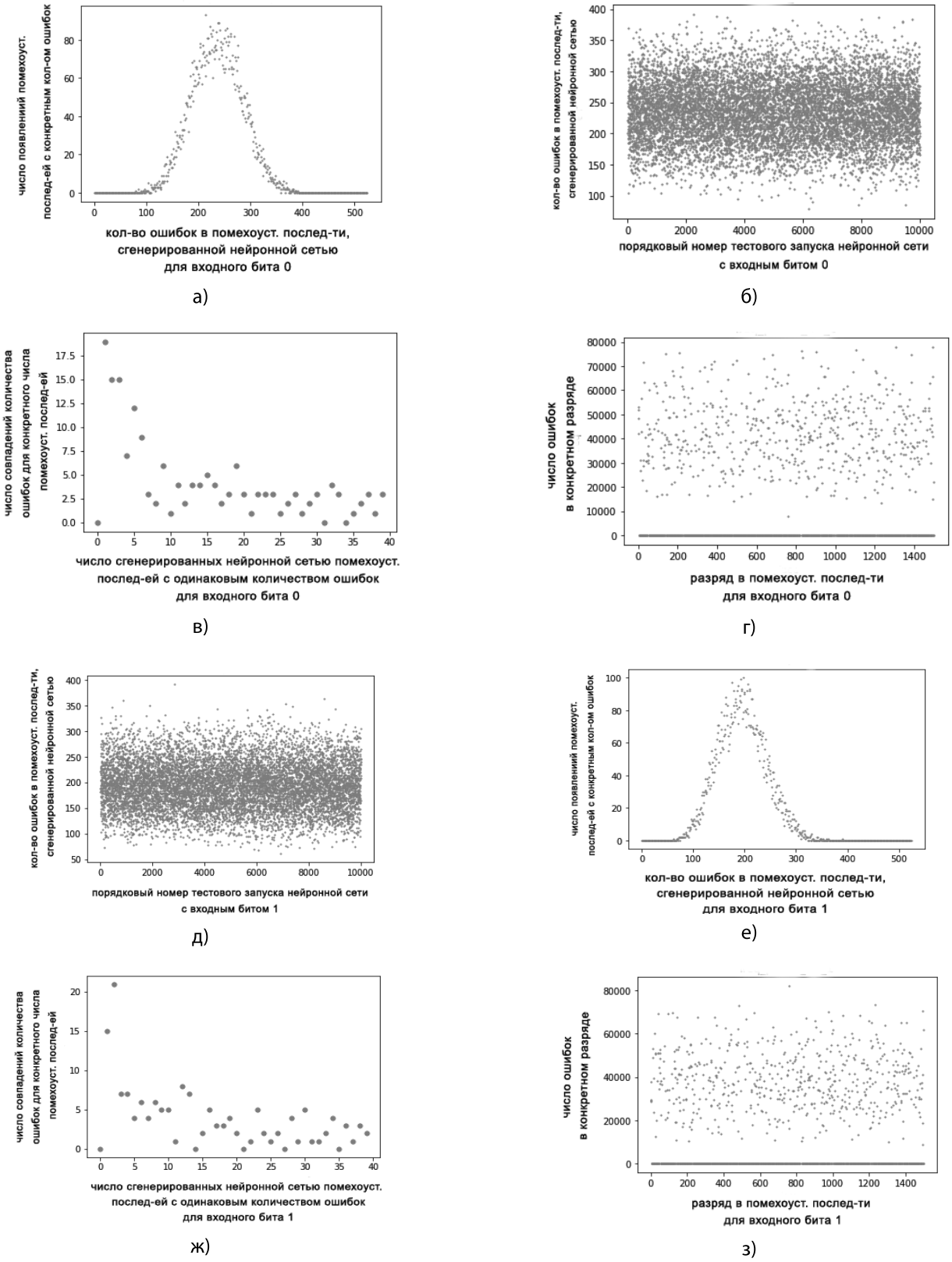


Рис. 4. Распределение ошибок в помехоустойчивых кодовых последовательностях, сгенерированных нейронной сетью

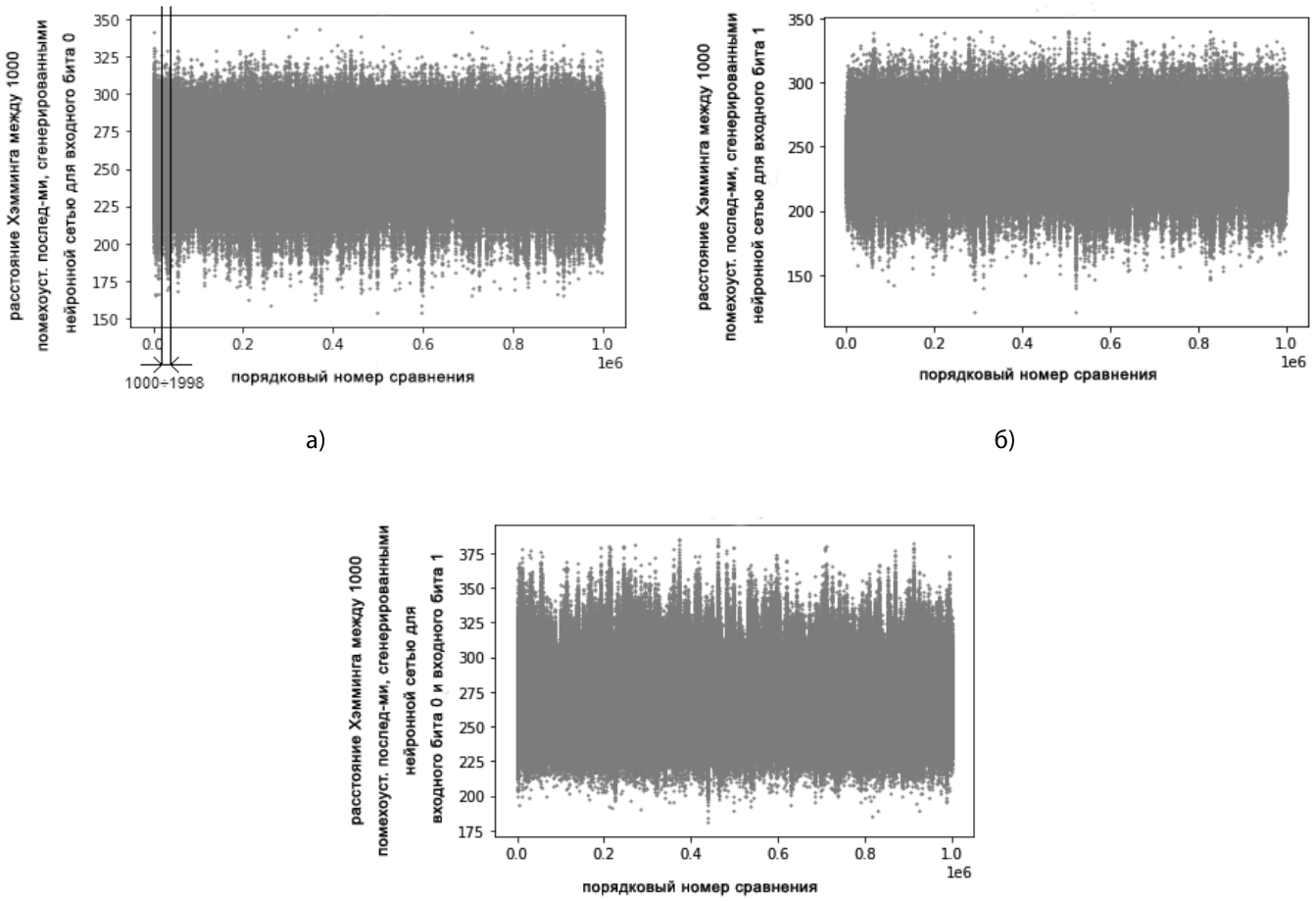


Рис. 5. Расстояние Хэмминга между сгенерированными нейронной сетью помехоустойчивыми кодовыми последовательностям

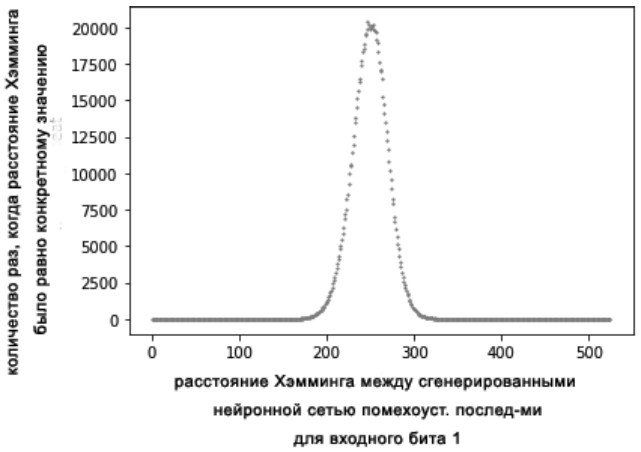
вательностями, соответствующим одной из M исходных последовательностей, и гиперпараметров нейронной сети [16], которыми являются размерность слоя $L1$, размерность слоя $L2$, интервал равномерного шума, вносимого при вычислении функции активации $ReLU\_noise$, и количества эпох обучения нейронной сети.

Для различных параметров системы, таких как размерность входных и выходных данных, количество классов исходных последовательностей и количество ошибок t, которые должна вносить нейронная сеть в N-битные помехоустойчивые кодовые последовательности, гиперпараметры нейронной сети подбирались экспериментально. Однако существуют и другие способы, позволяющие автоматизировать поиск гиперпарметров нейронной сети [17], а также методы их оптимизации [18].

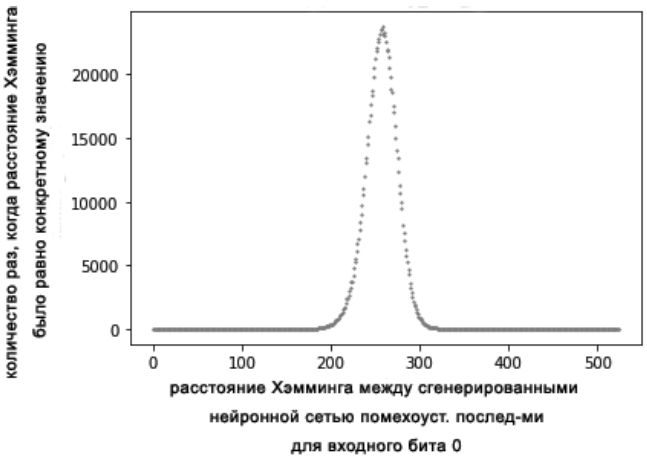
Пусть для двух исходных последовательностей, {0} и {1}, N = 1500 бит, t = 300, $d_{\min} \geq 601$. Тогда для нейронной сети, выступающей в качестве односторонней функции с секретом, необходимо выбрать следующие гиперпараметры: $k1$ = 0.3, $k2$ = 0.075, $noise$ = [–10.0; 10.0] для $ReLU\_noise$, количество эпох обучения равно 100.

10000 тестовых запусков нейронной сети показали следующие результаты. Для одной и той же исходной последовательности ({0} или {1}), поступающей на вход нейронной сети, на выходе из нейронной сети генерируется помехоустойчивая кодовая последовательность длиной 1500 бит, содержащая, не более чем t ошибок, где значения t изменяются согласно закону нормального распределения и в пределах дисперсии находятся в интервале ~ [200, 300] для исходной последовательности {0}, и ~[150, 250] для {1} (рис. 4).

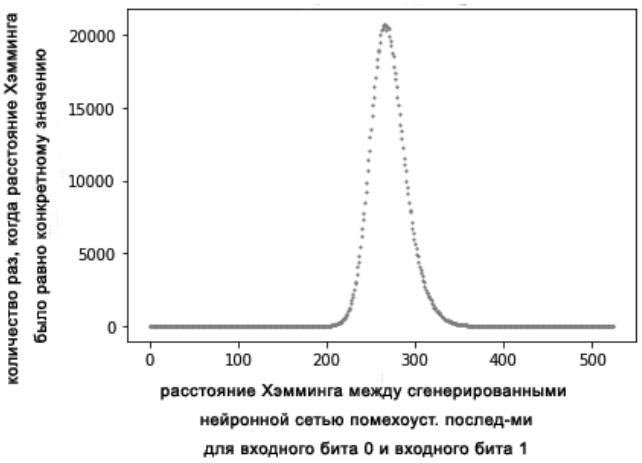
Собранная статистика по расстоянию Хэмминга для помехоустойчивых кодовых последовательностей с ошибками представлена на рисунке 5.



а)



б)



в)

Рис. 6. Распределение вероятностей значений расстояния Хэмминга для помехоустойчивых кодовых последовательностей, сгенерированных нейронной сетью

На рисунке 5(а) первые 999 значений — сравнение первой помехоустойчивой кодовой последовательностью, сгенерированной нейронной сетью, со всеми остальными. Значения с 1000 по 1998 — сравнение второй помехоустойчивой кодовой последовательностью, сгенерированной нейронной сетью, со всеми остальными и так далее.

На рисунке 5(б) — аналогично 5(а) для исходной кодовой последовательности {1}, поступившей на вход нейронной сети.

На рисунке 5(в) первые 999 значений — сравнение первой помехоустойчивой кодовой последовательностью, сгенерированной нейронной сетью для исходной кодовой последовательности {0}, со всеми помехоустойчивыми кодовыми последовательностями, сгенерированными нейронной сетью для исходной кодовой последовательности {1}. Значения с 1000 по 1998 — сравнение второй помехоустойчивой кодовой последовательностью, сгенерированной нейронной сетью для исходной кодовой последовательности {0}, со всеми помехоустойчивыми кодовыми последовательностями, сгенерированными нейронной сетью для исходной кодовой последовательности {1} и так далее.

Результаты анализа полученных данных показывают, что все три вышеперечисленных соотношения подчинены закону нормального распределения с близкими по значению математическим ожиданием [19] и дисперсией [20] (рис. 6).

В идеальном случае для вычисления прообраза односторонней функции с секретом необходимо пе-

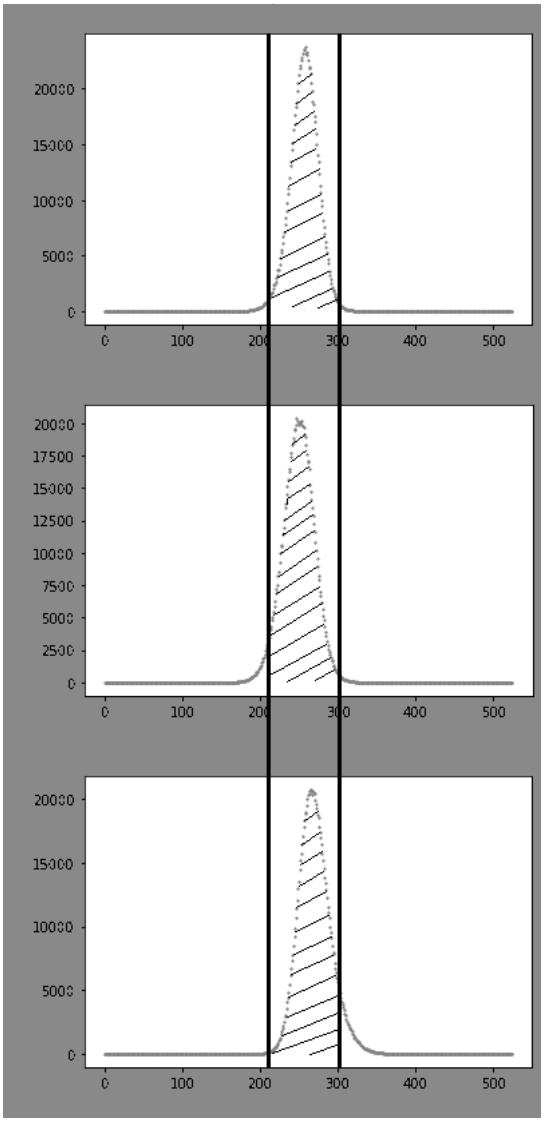


Рис. 7. Пересечение графиков нормального распределения расстояния Хэмминга для помехоустойчивых кодовых последовательностей, сгенерированных нейронной сетью

ребрать $(2^N)^2$ вариантов помехоустойчивых кодовых последовательностей. Однако на практике количество вариантов значительно меньше, так как в предлагаемой односторонней функции с секретом существует ограничение $d_{\min} \geq 2 \cdot t + 1$, то некоторые помехоустойчивые кодовые комбинации будут запрещенными. Количество таких комбинаций обозначим R_{comb}. Следовательно, количество возможных помехоустойчивых кодовых комбинаций из двух последовательностей длиной N равно $(2^N)^2 - R_{comb}$. Тогда количество разрешенных комбинаций, удовлетворяющих условию $d_{\min} \geq 2 \cdot t + 1$, будет равно $N_{allow} = N_{diff} \cdot 2^{2(N - d_{\min})}$, где N_{diff} — количество пар последовательностей длиной $d_{\min}$, в которых расстояние Хэмминга равно $d_{\min}$ — т.е. одна кодовая последовательность инверсна другой. Следовательно, $N_{diff} = 2^{d_{\min}}$.

Для N = 1500 бит, t = 300 количество вариантов, которые будет необходимо перебрать, будет равно

$$N_{diff} \cdot 2^{2(N - d_{\min})} = 2^{d_{\min}} \cdot 2^{2(N - d_{\min})} = 2^{2N - d_{\min}} = 2$$

$$= 2^{2 \cdot 1500 - 601} = 2^{2399} = 1.482 \cdot 10^{722}.$$

Однако, для обеспечения большей криптостойкости необходимо стремиться к выполнению условия $d_{\min} = 2 \cdot t + 1$:

$$N_{allow} = N_{diff} \cdot 2^{N - d_{\min}}.$$

$$N_{allow} = N_{diff} \cdot 2^{N - d_{\min}} = 2^{d_{\min}} \cdot 2^{N - d_{\min}} = 2^N = 2 \qquad 3.507\,10$$

$$= 2^{1500} = 3.507 \cdot 10^{451}.$$

Определим z как коэффициент, равный отношению площади под кривой на интервале, равном пересечению проекций на ось абцисс значений функций нормального распределения расстояния Хэмминга для помехоустойчивых кодовых последовательностей, сгенерированных искусственной нейронной сетью, к площади под кривой на интервале объединения проекций на оси абцисс (рис. 7).

Как видно из рисунка 7 площадь непересекаемых областей из трех графиков не превышает суммарно 10%, т.е. $z \approx 0.9$.

Данный факт означает, имеется возможность однозначно определять по N-битной помехоустойчивой кодовой последовательности с ошибками, сгенерированной нейронной сетью, исходную последовательность ({0} или {1}) в 10% процентах случаев.

Тогда для однозначного определения передаваемой последовательности длиной L бит, где, при $M = 2$, L — количество исходных комбинаций ({0} или {1}) переданных на вход нейронной сети, достаточно осуществить перебор 2^{L*z} вариантов комбинаций длиной L бит.

На классической вычислительной машине обучение нейронной сети, выполняющей обратное преобразование, является NP-полной задачей, так как обучаемой нейронной сети необходимо решать задачу декодирования произвольного кода. Необходимо отметить, что на данный момент не создан ни один квантовый алгоритм, способный обучить нейронную сеть, решающую NP-полную задачу за полиномиальное время, что в свою очередь позволяет сделать вывод о том, что предлагаемая односторонняя функция с секретом будет устойчива к определению прообраза на основе квантовых вычислений.

Заключение

Таким образом, искусственные нейронные сети с добавлением равномерного шума при вычислении значений функции активации для части нейронов сети в совокупности с помехоустойчивым кодированием способны выступать в качестве односторонней функции с секретом. При этом её стойкость к обратным вычислениям может быть подтверждена экспериментально для заданных исходных параметров нейронной сети.

Полученные теоретические и практические результаты также могут использоваться для модификации существующих методов криптографии, основанных на исправлении ошибок [21].

Криптосистема, основанная на предлагаемой односторонней функции с секретом, является системой, основанной на исправлении ошибок в помехоустойчивых кодах.

ЛИТЕРАТУРА

1. Garey, M.R.; Johnson, D.S. (1979). Computers and Intractability: A Guide to the Theory of NP-Completeness. New York: W.H. Freeman. ISBN.
2. Diffie, Whitfield; Hellman, Martin E. (November 1976). "New Directions in Cryptography". IEEE Transactions on Information Theory. 22 (6): 644–654. CiteSeerX 10.1.1.37.9720. doi:10.1109/TIT.1976.1055638. Archived from the original on 2014–11–29.
3. Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. 21 (2): 120–126. CiteSeerX 10.1.1.607.2677.
4. Politi, A; Matthews, J. C; O'Brien, J. L (2009). "Shor's Quantum Factoring Algorithm on a Photonic Chip". Science. 325 (5945): 1221. arXiv:0911.1242. Bibcode:2009Sci…325.1221P. doi:10.1126/science.1173731. PMID19729649. S2CID17259222
5. Mehlhorn, Kurt; Naher, Stefan (1990). "Bounded ordered dictionaries in O(log log N) time and O(n) space". Information Processing Letters. 35 (4): 183–189. doi:10.1016/0020–0190(90)90022-P.
6. Глава 2.5.2 Односторонняя функция // Приложение теории детерминированного хаоса в криптографии / Птицын Н. — 2002. с. 38–39.
7. Нефёдов В. Н., Осипова В.А. Курс дискретной математики.: МАИ, 1992. — 260 с.
8. Papadimitriou, Christos (1993). "Section 2.7: Nondeterministic machines". Computational Complexity (1st ed.). Addison-Wesley. pp. 45–50. ISBN.
9. Zell, Andreas (1994). Simulation Neuronaler Netze [Simulation of Neural Networks] (in German) (1st ed.). Addison-Wesley. p. 73. ISBN.
10. Вентцель Е. С., Овчаров Л.А. Теория случайных процессов и её инженерные приложения. — М., Наука, 1991. — с. 274.
11. Морелос-Сарагоса Р. 1.1.2. Хеммингово расстояние, Хемминговы сферы и корректирующая способность // Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В.Б. Афанасьева.: Техносфера, 2006. — С. 20–23. — (Мир связи). — 2000 экз. — ISBN5–94836–035–0.
12. Блейхут Р. Теория и практика кодов, контролирующих ошибки = Theory and Practice of Error Control Codes. —: Мир, 1986. — 576 с.
13. Hopfield, J. J. (1982). "Neural networks and physical systems with emergent collective computational abilities". Proceedings of the National Academy of Sciences. 79(8): 2554–2558. Bibcode:1982PNAS…79.2554H. doi:10.1073/pnas.79.8.2554. PMC346238. PMID6953413.
14. Ramachandran, Prajit; Barret, Zoph; Quoc, V. Le (October 16, 2017). «Searching for Activation Functions». ArXiv:1710.05941.
15. Han, Jun; Morag, Claudio (1995). "The influence of the sigmoid function parameters on the speed of backpropagation learning". In Mira, José; Sandoval, Francisco (eds.). From Natural to Artificial Neural Computation. Lecture Notes in Computer Science. 930. pp. 195–201. doi:10.1007/3–540–59497–3_175. ISBN.

16. Claesen, Marc & Bart De Moor (2015), Hyperparameter Search in Machine Learning, arXiv:1502.02127.
17. James Bergstra, Yoshua Bengio. Random Search for Hyper-Parameter Optimization // J. Machine Learning Research. — 2012. — Т. 13. с. 131–159.
18. Chris Thornton, Frank Hutter, Holger Hoos, Kevin Leyton-Brown. Auto-WEKA: Combined selection and hyperparameter optimization of classification algorithms // Knowledge Discovery and Data Mining. — 2013. — Bibcode: 2012arXiv1208.3719T. — arXiv:1208.3719.
19. Феллер В. Глава XI. Целочисленные величины. Производящие функции // Введение в теорию вероятностей и её приложения = An introduction to probability theory and its applications, Volume I second edition / Перевод с англ. Р.Л. Добрушина, А.А. Юшкевича, С.А. Молчанова Под ред. Е.Б. Дынкина с предисловием А.Н. Колмогорова. — 2-е изд. — М.: Мир, 1964. — С. 270–272.
20. Wasserman, Larry (2005). All of Statistics: a concise course in statistical inference. Springer texts in statistics. p. 51. ISBN9781441923226.
21. Dinh H., Moore C., Russell A. McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks (англ.) // Advances in Cryptology — CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14–18, 2011, Proceedings / P. Rogaway — Springer-Verlag, 2011. — P. 761–779. — 782 p. — ISBN978–3–642–22791–2 — doi:10.1007/978–3–642–22792–9_43.

Журнал «Современная наука: актуальные проблемы теории и практики»

г. Орел